King County	Department of Adult and Juvenile Detention All Divisions General Policy Manual	
	Chapter 1 **Administration and Personnel Management**	
1.02.015 - Multi-Factor Authentication	Approved By:	Director Allen Nance
	Effective Date:	August 26, 2025
	Reviewed By:	PRC
Distribution:	Review Date:	July 23, 2025

Purpose
To establish protocols for the use of multi-factor authentication and county issued authentication devices.

Policy
It is the policy of King County to require the use of multi-factor authentication to access King County information technology networks and assets.

References
DAJD Policies: 1.02.002 - Property Loss or Damage
DAJD Forms: Electronic Equipment Issue Agreement (F-681)
Officer's Report (F-627)
Staff Report

Definitions
Multi-Factor Authentication (MFA): A security technology that requires multiple methods of authentication before accessing information technology systems.
Multi-Factor Authentication (MFA) Device: An external device or hardware (i.e., smartphone, USB device, OATH token, etc.) used to authenticate permissions to access information technology systems.

A. General Guidelines

1. Employees must use a personal cell phone, a county-issued cell phone if provided to them, or other county-issued device equipped with Multi-Factor Authentication (MFA) software in order to access King County information technology (IT) systems and networks.
2. County-issued cell phones and other county-issued MFA devices are owned by King County and are provided to allow access to King County IT systems only.
3. MFA external devices are not to be loaned or transferred to another person.
4. Any violation of this policy may result in the MFA device being blocked from further use and access to county IT systems may be denied.
5. Employees will keep their assigned MFA device in good condition, with them at all times when working and in a secure location when not at work, as they would their access badge.
6. Employees will immediately report a lost, stolen or damaged MFA device or county

issued cellular phone to the chain of command via an Officer's Report (F-627) or Staff Report following department policy 1.02.002 - Property Loss or Damage.

7. Employees will also immediately report any lost, stolen or damage MFA or county issued cellular phone to King County Information Technology (KCIT).
   a. IT Help Desk Support Portal at https://helpdesk.kingcounty.gov.
   b. Telephone (206) 263-4357
8. There will be a **replacement fee** for any lost or damaged MFA device, if the damage was caused by the staff member's negligence or misuse.
9. If an employee's MFA device is stolen it must be reported, following department policy 1.02.002 - Property Loss or Damage.
10. Nonworking MFA devices will be replaced after the nonworking device has been turned into KCIT.
11. Employees shall return their issued MFA device upon request, separation from employment, or when they otherwise no longer meet MFA eligibility requirements.
12. Failure to return the issued MFA device will cause the device to be blocked from use and the replacement cost may be deducted from the employee's final compensation.